Remarks

In response to the Office Action mailed on July 13, 2007, the Applicants respectfully request reconsideration based on the following remarks. In the present application, the independent claims 15, 25, and 30 have been amended to specify the transmission a deactivation code and a passcode with the compressed image file, wherein the deactivation code comprises an instruction to the security office receiving the digital video image to end a current recording of the digital video image, wherein, in response to receiving the deactivation code, the passcode instructs the security office to delete the recorded digital video image if the passcode is determined to be valid, and wherein if the passcode is determined to be invalid, the digital video image is retained by the security office. Support for these amendments may be found in paragraphs 0054, 0055, and 0061 in the Specification. No new matter has been added.

Claims 15-36 are pending in the application. In the Office Action, claims 15-24 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Hoffberg (US 6,791,472) in view of Monroe et al. (US 7,023,913, hereinafter "Monroe") and Wenzel (US 6,513,119). Claims 25-34 and 36 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Hoffberg, Monroe, Wenzel, and further in view of Reynolds et al. (US 2004/0045030, hereinafter "Reynolds"). Claim 35 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Hoffberg, Monroe, Wenzel, Reynolds, and further in view of Stewart et al. (US 6,259,405).

Claim Rejections - 35 U.S.C. §103

Claims 15-24

Claims 15-24 stand rejected as being unpatentable over Hoffberg in view of Monroe and Wenzel. The rejection of these claims is respectfully traversed.

Amended independent claim 15 specifies a method for recording a digital video image. The method includes capturing a video image on a video-capture device; compressing the digital video image to create a compressed image file; transmitting the compressed image file over a wireless transmission channel using a real-time control protocol; retransmitting the compressed image file over a packet network to a security office, wherein the security office uses the digital video image to determine if assistance should be sent to a location of the capturing of the video image; and transmitting a deactivation code and a passcode with the compressed image file, wherein the deactivation code comprises an instruction to the security office receiving the digital video image to end a current recording of the digital video image, wherein, in response to receiving the deactivation code, the passcode instructs the security office to delete the recorded digital video image if the passcode is determined to be valid, and wherein if the passcode is determined to be invalid, the digital video image is retained by the security office.

It is respectfully submitted that the combination of Hoffberg, Monroe, and Wenzel and Shin fails to teach, disclose, or suggest each of the features specified in amended claim 15. For example, the aforementioned combination fails to disclose transmitting a deactivation code and a passcode with the compressed image file, wherein the deactivation code comprises an instruction to the security office receiving the digital video image to end a current recording of the digital video image, wherein, in response to receiving the deactivation code, the passcode instructs the security office to delete the recorded digital video image if the passcode is determined to be valid, and wherein if the passcode is determined to be invalid, the digital video image is retained by the security office.

Hoffberg discusses a mobile telecommunications device having a position detector, which may be absolute, relative or other type, a memory for storing events in conjunction with locations, and a transmitter or receiver for communicating information stored or to be stored in the memory. (See Hoffberg column 18, lines 17-21.) Hoffberg also discusses stored events that may be detected locally, such as through a detector for radar and/or laser emission source, radio scanner, traffic or road conditions (mechanical vehicle sensors, visual and/or infrared imaging, radar or LIDAR analysis, acoustic sensors, or the like), places of interest which may be selectively identified, itinerary stops, and/or fixed locations. (See Hoffberg column 19, lines 7-13.)

As conceded in the Office Action, Hoffberg fails disclose transmitting the compressed image file using a real time control protocol or a security office which uses the digital video image to determine if assistance should be sent to a location of the capturing of the video image. It is also submitted that Hoffberg fails to teach or suggest transmitting a deactivation code and a passcode with the compressed image file to stop a recording of the image, to delete the video image if the passcode is valid, and to retain the video image if the passcode is invalid. In contrast, Hoffman appears to be silent with respect to the transmission of codes for stopping the recording of an image and deleting an image received at a security office, as specified in amended claim 15.

Monroe, relied upon in the Office Action for allegedly curing the deficiencies of Hoffberg, discusses a digital security multimedia sensor which provides high resolution still image and/or streaming video signals via a network to a centralized, server supported security and surveillance system. A digital camera is adapted for collecting an image, compressing the image, and sending the compressed digital image signal to one or more receiving stations over a network. (See Monroe column 2, lines 35-49).

Monroe however, like Hoffman, appears to be silent with respect to the transmission of codes with a compressed image file for stopping the recording of an image and deleting an image received at a security office, as specified in amended claim 15. In contrast, Monroe merely discusses the collecting, compressing, and sending a digital image to a receiving station over a network.

Wenzel, relied upon in the Office Action for allegedly curing the deficiencies of Hoffberg, discusses an access security system in a gated community in order to overcome the drawbacks in conventionally guarded communities. (See Wenzel column 1, lines 33-36.) Wenzel discusses a central station CS that includes a first database DB1 for storing the visual data sent from the remote station RS and a second database DB2 for looking up historical data about a visitor V. (See Wenzel column 1, lines 33-36.)

As discussed in Applicants' previous Amendment filed on April 23, 2007, Wenzel fails to disclose transmitting the compressed image file using a real time control protocol. It is also submitted that Wenzel fails to teach or suggest transmitting a deactivation code and a passcode with the compressed image file to stop a recording of the image, to delete the video image if the passcode is valid, and to retain the video image if the passcode is invalid. In contrast, Wenzel appears to be silent with respect to the transmission of codes for stopping the recording of an image and deleting an image received at a security office, as specified in amended claim 15.

Based on the foregoing, the combination of Hoffberg, Monroe, and Wenzel fails to teach, disclose, or suggest each of the features specified in amended claim 15. Therefore, claim 15 is allowable and the rejection of this claim should be withdrawn. Claims 16-24 depend from amended claim 15 and are thus allowable for at least the same reasons. Therefore, the rejection of these claims should also be withdrawn.

Claims 25-34 and 36

Claims 25-34 and 36 stand rejected as being unpatentable over Hoffberg, Monroe, Wenzel, and further in view of Reynolds. The rejection of these claims is respectfully traversed.

Amended independent claims 25 and 30 specifies similar features as amended claim 15 and are thus allowable over the combination of Hoffberg, Monroe, and Wenzel for at least the same reasons. Reynolds, relied upon in the Office Action for allegedly curing the deficiencies of Hoffberg, Monroe, and Wenzel, discusses streaming media communication between a transmission device and one or more destination devices. The media communication may be compressed and decompressed using a CODEC. (See Reynolds paragraphs 0149-0160).

Reynolds however, fails to teach or suggest transmitting a deactivation code and a passcode with the compressed image file to stop a recording of the image, to delete the video image if the passcode is valid, and to retain the video image if the passcode is invalid, as specified in amended claims 25 and 30. In contrast, Reynolds appears to be concerned with compression and not the transmission and use of the aforementioned codes.

Based on the foregoing, the combination of Hoffberg, Monroe, Wenzel, and Reynolds fails to teach, disclose, or suggest each of the features specified in amended claims 25 and 30. Therefore, claims 25 and 30 are allowable and the rejection of these claims should be withdrawn. Claims 26-29, 31-34, and 36 depend from amended claims 25 and 30 and are thus allowable for at least the same reasons. Therefore, the rejection of these claims should also be withdrawn.

Claim 35

Claim 35 stands rejected as being unpatentable over Hoffberg, Monroe, Wenzel, Reynolds, and further in view of Stewart. The rejection of this claim is respectfully traversed.

Claim 35 depends from amended independent claim 30 and thus specifies at least the same features. As discussed above, the combination of Hoffberg, Monroe, Wenzel, and Reynolds fails to teach, disclose, or suggest transmitting a deactivation code and a passcode with the compressed image file to stop a recording of the image, to delete the video image if the passcode is valid, and to retain the video image if the passcode is invalid, as specified in claim 35. Stewart, relied upon in the Office Action for allegedly curing the deficiencies of Hoffberg, Monroe, Wenzel, and Reynolds, discusses a geographic-based communications service system which receives user identification information from a user device. Upon receipt of the user identification information, the system may transmit the information and a known geographic location of an access point in communication with the user device, to one or more network providers. The geographic location may be used by a network provider to provide selected content information (e.g., reservation information and messaging information) to a desired recipient. (See Stewart column 2, line 39 through column 4, line 6).

Steward however, fails to teach or suggest transmitting a deactivation code and a passcode with the compressed image file to stop a recording of the image, to delete the video image if the passcode is valid, and to retain the video image if the passcode is invalid, as specified in claim 35. In contrast, Stewart appears to be concerned with user identification information for use in determining a geographic location of a user communication device.

Based on the foregoing, the combination of Hoffberg, Monroe, Wenzel, Reynolds, and Stewart fails to teach, disclose, or suggest each of the features specified in amended claim 35. Therefore, claim 35 is allowable and the rejection of this claim should be withdrawn for at least the foregoing reasons.

Conclusion

In view of the foregoing amendments and remarks, this application is now in condition for allowance. A notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is invited to call the Applicants' attorney at the number listed below.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 13-2725.

Respectfully submitted,

MERCHANT & GOULD P.C.
P.O. Box 2903
Minneapolis, Minnesota 55402-0903
(404) 954-5064

Date: January 14, 2008

/Alton Hornsby III/
Alton Hornsby III
Reg. No. 47,299

39262
PATENT TRADEMARK OFFICE